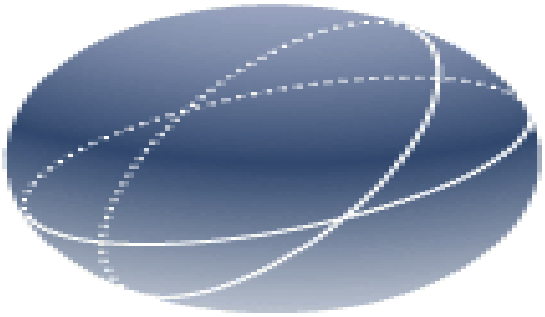
MARIA ONILDE CARDOSO FERNANDES

Equações em Z e suas Resoluções



Licenciatura em Matemática

ISE, Setembro de 06

INSTITUTO SUPERIOR DE EDUCAÇÃO

DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

Trabalho Científico

apresentado ao ISE para obtenção do grau de Licenciatura em Matemática

Sob orientação de Dra. Tetyana Gonçalves

Ministério da Educação e Ensino Superior
Instituto Superior de Educação

Departamento de Ciência e Tecnologia

CURSO DE MATEMÁTICA

Trabalho Cientifico

Equações em Z e suas resoluções

Elaborado por: Maria Onilde Cardoso Fernandes
e aprovado pelos membros do júri.

Foi homologado pelo concelho científico-pedagogico com requisito parcial à obtenção do grau de licenciatura em Matemática

Data _____/_____/_____

Júri,

_____

_____

_____

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus pela vida, saúde, força e coragem.
Do mesmo modo queria deixar expresso os meus agradecimentos a todos aqueles que de uma forma ou doutra contribuíram para que hoje possa apresentar este trabalho, nomeadamente os meus pais Cândido Fernandes e Maria dos Reis Cardoso, meus irmãos Silvestre Fernandes, Carlos Fernandes, Filomeno Fernandes e Orlando Fernandes, minhas irmãs Filomena Cardoso, Aguinalda Cardoso, Cesaltina Cardoso e Elisia Cardoso, meus professores, amigos e colegas principalmente Nelson Barros, Elisa Tavares, António Barradas e Palmira Cabral.

Um especial agradecimento vai para a professora Dra. Tetyana Gonçalves pelos apoios, orientação ao longo dos tempos.

A todos, muito obrigada

Setembro de 2006

Maria Onilde Cardoso Fernandes

ÍNDICE

I

INTRODUÇÃO

Ao longo da história da matemática, encontramos várias referências a matemáticos que estudaram métodos de resolução de equações.

De entre esses métodos encontramos o método sobre a equação equivalente em que o famoso matemático Al-khawrsmi chamou aljebr, donde resultou a palavra álgebra que é o ramo da matemática que trata, entre outros assuntos, bem como da resolução de equações.

Chamamos equação algébrica de grau n ≥2 à uma igualdade

$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0$,

onde $a_i \in R(i = \overline{0,n}), a_n \neq 0,$

Procura-se determinar os números x, a ´´incognita ``, de modo que a igualdade seja satisfeita.

O presente trabalho é dedicado ao estudo de alguns método de resolução de equações algébricas.

Este campo de investigação é vastíssimo, sendo assim, não podendo abranger todos os casos possíveis, concentramo-nos nos aspectos ligados com a resolução de equações sobre Q (corpo dos números racionais) e Z (anel dos números inteiros), nomeadamente, com as equações de Diofanto, de Pitágoras e de Fermat.Um dos métodos utilizados na resolução de tais equações baseia-se na ´´teoria das fracções continuas finitas e infinitas ``(estudada na cadeira de ´´teoria dos Números``). Por isso, o segundo capítulo dedica-se à breve revisão dos conceitos necessários que facilitam a leitura e compreensão da monografia. Pressupõe-se, também, que o leitor domina os conceitos da ´´teoria de divisão em Z``e ´´teoria das congruências ``, e tem conhecimentos básicos da ´´geometria analítica``.

Em termos metodológicos, para elaboração deste trabalho procedeu-se a análise de alguns livros, bem como pesquisas em Internet, para que possamos apresentar um estudo mais completo. Recorda-se, que os manuais consultados, são bastantes escassos, pelo que tivemos de fazer um esforço muito grande.

Neste trabalho usam-se, entre outras, as seguintes designações especiais:

I é a designação do primeiro capítulo;

II é a designação do segundo capítulo;

… …

2.1 é a designação do primeiro parágrafo do capitulo II;

3.3 é a designação do terceiro parágrafo do capitulo III

… …

As definições, teoremas, lemas, corolários têm enumeração própria em cada capítulo.

Por exemplo:

Teorema 5.2.1 é o primeiro teorema do segundo parágrafo do capítulo V;

Definição 4.1 é a designação da primeira definição do capítulo IV;

… …

As enumerações das fórmulas são feitas por capítulos.

II

CONCEITOS PRELIMINARES

2.1-FRACÇOES CONTINUAS ARITMÉTICAS

Definição 2.1.1. Ao número escrito sob a forma:

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ldots}}} \qquad (1)$$

$$+\cfrac{1}{a_{s-1}+\cfrac{1}{a_s}}$$

onde $a_0, a_1, a_2, ..., a_{s-1}, a_s$ são números inteiros tais que:

$a_1 \geq 1, a_2 \geq 1, ..., a_{s-1} \geq 1, a > 1$, chama-se **fracção contínua finita**

OBS: Se s=0, $a_s = a_0$ é um número inteiro.

Podemos também escrever (1) sob a forma $[a_0; a_1, a_2, ..., a_s]$.

Aos números $a_0, a_1, a_2, ..., a_{s-1}, a_s$ vamos chamar de elementos de fracção contínua com parte inteira igual a a_0.

Teorema 2.1.1. Todo o número racional pode ser representado sob a forma de fracção contínua (1).

Teorema2.1.2. Para todo o número racional existe uma única fracção contínua que o representa.

Os **teoremas 2.1.1** e **2.1.2** estabelecem uma relação biunívoca entre os números racionais e as fracções contínuas finitas.

Caso o número seja irracional, o processo descrito acima não termina para nenhum a_i inteiro.Em consequência os números irracionais darão origem a expressões infinitas do tipo:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_i + \ddots}}}$$

em que todos os a_i $i \in N$ são números inteiros e todos os $a_i, (i \in N \setminus \{0\})$ são positivos

.

2.2-FRACÇOES PRÓXIMAS

Se truncarmos uma fracção contínua no termo a_i obtivemos sua i^{essima} fracção reduzida (fracção próxima):

$$R_i = a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_i}}$$

Lema 2.2.1. As fracções próximas de ordem ímpar (par) aproximam a fracção original por excesso (por falta).

Para uma fracção contínua:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_{s-1} + \cfrac{1}{a_s}}}}} \qquad (1)$$

Consideram-se as fracções próximas:

$$A_0 = a_0, A_t = a_0 + \frac{1}{a_1}, A_2 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}, ...,$$

$$A_s = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_{s-1} + \cfrac{1}{a_s}}}}}$$

Definiçao2.2.1. A n-ésima fracção próxima ($0 \le n \le s$) para uma fracção contínua finita (1) é da forma

$$A_n = a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_n}} \qquad (2)$$

Consideremos agora duas sucessões de números:

$P_0, P_1, ..., P_s$ *e* $Q_{0,} Q_{1,...,} Q_S$, definidas por recorrência ,pondo

$$P_n = P_{n-1} a_n + P_{n-2}$$
$$Q_n = Q_{n-1}.a_n + Q_{n-2} \qquad (2 \le n \le s) \qquad (3)$$

Com condições iniciais:

$$P_0 = a_0\ , Q_0 = 1, P_1 = a_0.a_1 + 1, Q_1 = a_1 \qquad (4)$$

É fácil ver que (3) e (4) determinam univocamente os números $P_0, P_1, ..., P_s$ *e* $Q_{0,} Q_{1,...,} Q_S$ a partir dos elementos $a_0, a_1, a_2, ..., a_{s-1}, a_s$.

Teorema 2.2.1. Se $a_0, a_1, a_2, ..., a_{s-1}, a_s$ são elementos da fracção contínua (1), então a sucessão de números $P_0, P_1, ...P_s, Q_0, Q_1, ...Q_s$ definidas pelas fórmulas (3) e (4) tem a propriedade seguinte:

Para todo n (n=0..s) o número racional $\frac{P_n}{Q_n}$ é a n-ésima fracção próxima (2).

Definição 2.2.2. Aos números $P_n, Q_n \ \left(n = \overline{o,s}\right)$ definidos pelas fórmulas (3) e (4) chamam-se, respectivamente, numeradores e denominadores das fracções próximas à fracção contínua (1).

Obs: O cálculo dos numeradores P_n e denominadores Q_n das fracções próximas é conveniente realizar pelo esquema seguinte:

	a_0	a_1	a_2	…	a_s
P_n	a_0	a_0a_1+1	$\left(a_0a_1+1\right)a_2+a_0$	…	…
Q_n	1	a_1	a_1a_2+1	…	…

As fracções próximas, seus numeradores e denominadores possuem as propriedades seguintes:

Teorema 2.2.2. Para $n = \overline{0,s}$ tem lugar a igualdade seguinte:

$$P_nQ_{n-1} - P_{n-1}Q_n = (-1)^{n-1} \qquad (6)$$

Teorema 2.2.3. O numerador e o denominador de uma fracção próxima são números primos entre si.

Teorema 2.2.4. Para $1 \le n \le s$ se tem:

$$(i) \quad \frac{p_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^{n-1}}{Q_nQ_{n-1}}; \qquad (7)$$

$$(ii) \quad \left|\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}}\right| = \frac{1}{Q_nQ_{n-1}}. \qquad (8)$$

Teorema 2.2.5. **O**s denominadores das fracções próximas à fracção contínua (1) formam uma sucessão monótona crescente, começando de Q_0, isto é:

$$1 = Q_0 \le Q_1 < Q_2 < \ldots < Q_s.$$

Teorema 2.2.6. Para $n \ge 2$ se tem:

$$P_n Q_{n-2} - P_{n-2} Q_n = (-1)^n a_n \qquad (10)$$

Teorema 2.2.7. Ás fracções próximas pares (com índices pares) formam uma sucessão crescente e as fracções próximas impares (com índices ímpares) formam uma sucessão decrescente.

Definição 2.2.3. Ás duas fracções próximas $\frac{p_{n-1}}{Q_{n-1}} e \frac{P_n}{Q_n}$ de índices sucessivos vamos chamar de ***fracções – vizinhas*****.**

Teorema2.2.8. De duas fracções – vizinhas a fracção de índice par é sempre menor do que fracções de índice ímpar.

Teorema2.2.9. Uma fracção próxima de índice par é menor do que uma fracção próxima de índice ímpar.

Teorema 2.2.10. As distancias entre fracções próximas – vizinhas diminuem-se com o aumento dos seus índices.

Teorema 2.2.11. Sejam P_i, Q_i fracções próximas à $[a_0; a_1, \ldots a_s]$ (desenvolvimento do número

A em fracção contínua) tem lugar a desigualdade seguinte:

$$0 < P_{2n-1} - AQ_{2n-1} < \frac{1}{Q_{2n}}$$

Demonstração . Seja A um número real não inteiro.

Sabendo que as fracções próximas (R_n) de ordem ímpar excedem A.

Portanto

$$\mathrm{A} < R_{2n-1} = \frac{P_{2n-1}}{Q_{2n-1}}$$

$$\mathrm{A} < \frac{P_{2n-1}}{Q_{2n-1}}$$

$$AQ_{2n-1} < P_{2n-1}$$

$$0 < P_{2n-1} - AQ_{2n-1}$$

donde se reduz a primeira desigualdade do teorema.

Por outro lado vimos que A excede as fracções próximas de ordem par.

Então

$$R_{2n} < \mathrm{A}$$

que implica

$$R_{2n-1} - A < R_{2n-1} - R_{2n}$$

Atendendo ao **teorema 2.2.4 – (i)** podemos escrever

$$R_{2n-1} - A < \frac{1}{Q_{2n}Q_{2n-1}}$$

ou $$\frac{P_{2n-1}}{Q_{2n-1}} - A < \frac{1}{Q_{2n}Q_{2n-1}}$$

Multiplicando por Q_{2n-1} obtemos a segunda desigualdade do teorema.

III

EQUAÇÕES DE DIOFANTO

3.1- CONSIDERAÇOES GERAIS

Definição 3.1.1. À equação linear de n incógnitas da forma

$$a_1x_1 + a_2x_2 + ... + a_nx_n = b \qquad (1)$$

onde todos os coeficientes e incógnitas são números inteiros e, pelo menos, um $a_i \neq 0, i = \overline{1,n}$, chama-se ***diafantina*** (equação de Diofanto).

A solução da equação (1) é n-uplo ordenado $\left(x_1', x_2', ..., x_n'\right)$ que a satisfaz.

Teorema 3.1.1. Se os coeficientes de (1) são primos entre si então $a_1x_1 + a_2x_2 + ... + a_nx_n$ =1 tem uma solução em Z.

Demonstração. Designemos por M o conjunto de tais números inteiros positivos b para os quais (1) tem soluções em Z. M, evidentemente, não é vazio, pois para $a_1x_1 + a_2x_2 + ... + a_nx_n$ for um número positivo.

Em M existe o número mínimo (**teorema** – Cada subconjunto (não vazio) de N contem número mínimo), designemo-lo por d ($d \in M$).

Sejam $x_1', x_2', ..., x_n'$ são inteiros tais que

$a_1x_1' + a_2x_2' + ... + a_nx_n'$ =d e $a_1 = dq + r$, onde $0 \le r <$d então

$$r = a_1 - \left(a_1x_1' + a_2x_2' + ... + a_nx_n'\right)q = a_1\left(1 - qx_1'\right) + a_2\left(-qx_2'\right) + ... + a_n\left(-qx_n'\right)$$

Desse modo, encontramos os valores inteiros: $x_1 = 1 - qx_1', x_2 = -qx_2', ..., x_n = -qx_n'$, tais que $a_1x_1 + a_2x_2 + ... + a_nx_n$ = r, mas $0 \le r <$de d é o mínimo positivo em M, isto é r não pode ser um número positivo e tem que ser somente igual a zero (r = 0), logo,

$a_1 = dq, d \mid a_1$.Analogamente, $d \mid a_2, ..., d \mid a_n$.

Portanto, d é divisor comum dos números $a_1, a_2, ..., a_n$. Assim como ($a_1, a_2, ..., a_n$) =1,d|1 e d=1,1 $\in M$,isto é $a_1x_1 + a_2x_2 + ... + a_nx_n = b$ é resolúvel em Z.

Teorema3.1.2. Seja d é M.D.C ($a_1, a_2, ..., a_n$). A equação (1) tem soluções se e somente se d|b. A quantidade de soluções de (1) é igual a zero ou é infinita ((1) é indeterminado).

Demonstração. Consideremos todos os três casos:

(i) Seja d|b. Para a equação

$$\frac{a_1}{d}x_1 + \frac{a_2}{d}x_2 + ... + \frac{a_n}{d}x_n = 1,$$

onde ($\frac{a_1}{d}, \frac{a_2}{d}, ..., \frac{a_n}{d}$) =1,existem números inteiros $c_1, c_2, ..., c_n$ que a satisfazem (**teorema 3.1.1**), isto é.

$$\frac{a_1}{d}c_1 + \frac{a_2}{d}c_2 + ... + \frac{a_n}{d}c_n = 1$$

Então

$$a_1\left(c_1\frac{b}{d}\right) + a_2\left(c_2\frac{b}{d}\right) + ... + a_n\left(c_n\frac{b}{d}\right) = b$$

Isto é $\left(c_1\frac{b}{d}, c_2\frac{b}{d}, ..., c_n\frac{b}{d}\right)$-solução de (1).

(ii) Seja d não divide b. Então a parte esquerda de (1) se divide por d, para quaisquer valores inteiros de $x_1, x_2, ..., x_n$, mas a parte direita não se divide por d. Logo a igualdade (1) é impossível para inteiros $x_1, x_2, ..., x_n$,

(iii) Se ($x_1', x_2', ..., x_n$) satisfaz a (1) então, por exemplo, todos os n-uplos ordenados ($x_1' + a_2 t, x_2' - a_1 t, x_3', ..., x_n$) para $t \in Z$, também satisfazem a (1). Portanto a equação (1) ou não tem soluções, ou é indeterminada.

Exemplos:

1) $10x_1 - 20x_2 + 15x_3 = 112$ não tem soluções ,pois d=5 e 5 não divide 112.

2) $21x_1 + 5x_2 - 18x_3 + 36x_4 = 10$ é indeterminado,pois d=1 .

3.2-EQUAÇOES DA FORMA ax+by=c COM a, b, c $\in Z$

Definição 3.2.1. À equação da forma ax+by=c, (2)
onde a, b, c, x, y $\in$ Z, chama-se diafantina de duas incógnitas.

Teorema3.2.1. Seja (a,b)=d, onde a≠0,b≠0,d|c e (x_0, y_0) uma solução de (2) .Então o conjunto de soluções de (2) em Z coincide com o conjunto de pares (x', y'),tais que

$$x' = x_0 - \frac{b}{d}.t \; ; \; y' = y_0 + \frac{a}{d}.t \quad , t \in Z.$$

Demonstração. Pela hipótese x_0, y_0 , satisfazem a equação (2), isto é

$$ax_0 + by_0 = c. \qquad (2')$$

Seja (x´,y´)uma solução qualquer de (2) ,isto é

$$ax' + by' = c \qquad (3)$$

Subtraindo de (2´) -(3) e dividindo ambas as partes da igualdade obtida por d,teríamos :

$$\frac{a}{d}(x_0 - x') + \frac{b}{d}(y_0 - y') = 0$$

$$\frac{a}{d}(x_0 - x') = \frac{b}{d}(y' - y_0), onde\ \frac{a}{d}, \frac{b}{d} \in Z.$$

Então, assim como $(\frac{a}{d}, \frac{b}{d}) = 1$ (**propriedade** -Se $(a_1, ..., a_n) = d$ então $\left(\frac{a_1}{d}, ..., \frac{a_2}{d}\right) = 1$)

$\frac{a}{d} | (y' - y_0)$ (**propriedade**- $se\ c | ab\ e\ (a,c) = 1$ então $c | b$), isto é

$\exists t \in Z : y' = y_0 + \frac{a}{d}.t$

(**definição** – Sejam a,bЄZ(b≠0),chama-se divisor de a se existe q ЄZ: a=bq). De (3) temos:

$ax' = c - by' = c - b(y_0 + \frac{a}{d}.t) = (c - by_0) - \frac{ab}{d}.t = ax_0 - \frac{ab}{d}.t, de\ \ onde\ \ vem\ \ x' = x_0 - \frac{b}{d}.t$

Sendo assim, qualquer solução de (2) terá a forma:

$$x' = x_0 - \frac{b}{d}.t$$

$$y' = y_0 + \frac{a}{d}.t \quad , t \in Z.$$

A afirmação inversa também é verdadeira. Realmente, se (x´,y´)tal que

$x' = x_0 - \frac{b}{d}.t$, $y' = y_0 + \frac{a}{d}.t$, $t \in Z$,então

$a\left(x_0 - \frac{b}{d}.t\right) + b\left(y_0 + \frac{a}{d}.t\right) = ax_0 + by_0 = c$,isto é (x´,y´) é uma solução de (2).

OBS: O teorema é verdadeiro para a=0 ou b=0.

Se a=0, então by=c ,onde (0,b)=d=b e quando b|c para y se tem o valor único $y_0 = \frac{c}{b}, x \in Z$.

Logo, qualquer solução pode ser escrita sob a forma:

$x' = x_0 - 1.t$, $y' = y_0 + 0.t$ $, t \in Z$ e tais x´,y´ satisfazem a equação 0x+by=c.

Para resolver a equação ax+by=c ,(a,b)=1 em números inteiros é preciso encontrar uma solução particular (x_0, y_0).Podemos fazer isso,utilizando a decomposição do número $\frac{a}{b}$ em fracção contínua finita .

Com efeito, se $\frac{a}{b} = [a_0; a_1, a_2, ..., a_s]$ e $\frac{p_n}{Q_n}\left(n = \overline{0, s}\right)$ fracções próximas à fracção contínua $[a_0; a_1, a_2, ..., a_s]$, então $\frac{a}{b} = \frac{P_s}{Q_s}$.

Pelo **teorema 2.2.2**: $P_s Q_{s-1} - P_{s-1} Q_s = (-1)^{s-1}$ isto é $aQ_{s-1} - bP_{s-1} = (-1)^{s-1}$.

Multiplicando ambas as partes da última igualdade por $(-1)^{s-1} c$, obtemos: $a((-1)^{s-1} Q_{s-1} c) + b((-1)^s P_{s-1} c) = c$ isto é

$x_0 = (-1)^{s-1} Q_{s-1} c$, $y_0 = (-1)^s P_{s-1} c$ satisfazem a equação (2)para (a,b)=1,

Quer dizer $\left((-1)^{s-1} Q_{s-1} c, (-1)^s P_{s-1} c\right)$ é a solução particular de (2).Desse modo, tem lugar:

<u>Teorema 3.2.2.</u> A solução qualquer, em Z, da equação diafantina ax+by =c, onde a,b,c$\in Z$ e (a,b)=1,representa-se sob a forma :

$$\begin{aligned} x &= (-1)^{s-1} Q_{s-1} c - bt, \\ y &= (-1)^s P_{s-1} c + at, \qquad t \in Z \end{aligned} \tag{4}$$

Onde P_{s-1}, Q_{s-1} numerador e denominador da penúltima fracção próxima à fracção contínua $\frac{a}{b} = [a_0; a_1, a_2, ..., a_s]$.

Exemplo:

Resolver a equação seguinte em Z:

19x+7y=3.

$$\frac{19}{7}=[2;1,2,2]\ e\ \frac{P_n}{Q_n}:\frac{2}{1},\frac{3}{1},\frac{8}{3},\frac{19}{7},\ onde\ \frac{P_2}{Q_2}=\frac{8}{3}$$

$$Por\ (4): x=(-1)^2.3.3-7t,$$

$$y=(-1)^3.3.8+19t \qquad t\in Z$$

Ao nível do Ensino Secundário, sem introdução do conceito de ´´fracção continua ``é possível resolver equações desse tipo dos modos seguintes:

Sendo (19,7)=1 então existe solução x,y$\in$ Z tal que :

-

$$7y=3-19x \Leftrightarrow y=\frac{3-19x}{7}\in Z$$

$$y=\frac{3-(14x+5x)}{7}=-2x+\frac{3-5x}{7}$$

$$\frac{3-5x}{7}\in Z \Leftrightarrow \frac{3-5x}{7}=t\Rightarrow 3-5x=7t\Leftrightarrow x=\frac{3-7t}{5}\Leftrightarrow$$

$$\Leftrightarrow x=-t+\frac{3-2t}{5},\Rightarrow \frac{3-2t}{5}=k\in Z\Rightarrow$$

$$\Rightarrow 3-2t=5k\Leftrightarrow \frac{3-5k}{2}=t\Rightarrow t=-2k+\frac{3-k}{2}\Rightarrow$$

$$\Rightarrow \frac{3-k}{2}=u\in Z\Rightarrow k=3-2u$$

$$Logo, t=\frac{3-5(3-2u)}{2}=\frac{3-15+10u}{2}=\frac{-12+10u}{2}=-6+5u$$

$$x=\frac{3-7(-6+5u)}{5}=\frac{3+42-35u}{5}=\frac{45-35u}{5}=9-7u,\quad u\in Z$$

$$y=\frac{3-19(9-7u)}{7}=\frac{3-171+133u}{7}=\frac{-168+133u}{7}=-24+19u, u\in Z$$

-

19=7.2+5

7=5.1+2

5=2.2+1

2=2.1

$\exists u, v \in Z : 19u + 7v = 1$

1=5-2.2=5-2(7-5.1) =5-2.7+2.5=

=-2.7+3.5=-2.7+3(19-7.2) =

=-2.7+3.19-6.7=19.3-7.8=19.3+7.(-8)

Isto é

19.3+7.(-8) =1

$19.(3.3) + 7(-8.3) = 3$

$\downarrow \quad \downarrow$

$x_0 \quad y_0$

$\Downarrow$

$x_0 = 9$

$y_0 = -24$

$\Rightarrow x = x_0 - bt$

$y = y_0 + at$

$\Rightarrow x = 9 - 7t,$

$y = -24 + 19t, \quad t \in Z$

- Ainda pode-se resolver a mesma equação graficamente, dando os seguintes

passos:

1º Resolver a equação em ordem a uma das variáveis (y);

2º Representar graficamente a expressão obtida;

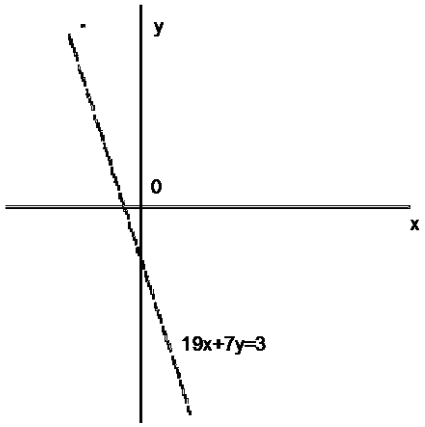
3º Concluir que a equação tem uma infinidade de soluções e que essas soluções são todos os pontos da recta que a expressão representa.

De acordo com os passos apresentados, eis o exemplo:

Resolvendo em ordem a y temos:

$$y = \frac{3-19x}{7}$$

A expressão $y = \frac{3-19x}{7}$ representa uma recta (gráfico de uma função afim)



A equação 19x+7y=3 tem infinitas soluções:

(2,5); (9, -24); …

Todos os pontos da recta $y = \frac{3-19x}{7}$ são soluções da equação

IV

EQUAÇÕES DE PITÁGORAS DO TIPO $X^2+Y^2=Z^2$

O matemático grego Pitágoras sabia resolver equações da forma

$$X^2+Y^2=Z^2 \qquad (1)$$

em números inteiros Z

Para isso utilizava interpretações geométricas e aritméticas.

4.1 – CONSIDERAÇÕES GERAIS

Uma das interpretações geométricas incide com triângulo rectângulo de catetos X e Y e hipotenusa Z que satisfazem ao teorema de Pitágoras (quadrado da hipotenusa é igual a soma dos quadrados dos catetos) $X^2+Y^2=Z^2$ cujos lados têm medidas inteiras.

Desde antigamente sabemos um exemplo dos números X, Y, Z que satisfazem a equação (1):

X=3,Y=4, Z=5.

Devido a esta interpretação um trio (X, Y, Z) de números naturais satisfazendo $X^2+Y^2=Z^2$ diz – se um **trio pitagórico** ou «troica**» pitagórica**.

Descrevendo todas as troicas pitagóricas isto é triplos ordenados (X, Y, Z) dos inteiros que satisfazem a equação (1)

Observemos, primeiro, que tendo uma «troica» que satisfaz a equação (1), por exemplo, (x_0, y_0, z_0) qualquer outra da forma $(kx_0, ky_0, kz_0)k \in Z$ também satisfaz (1)

Por isso basta encontrar só «troicas» dos números primos (entre si) em pares, pois se quaisquer dois números entre x, y, z se dividem por um número primo p, então o terceiro também se divide por p.

Definição 4.1.1. Um trio pitagórico cujos elementos são primos entre si diz-se **primitivo.**

Claramente, basta procurar os trios pitagóricos primitivos.

Vamos de seguida ver uma consequência de condições que tais trios têm a satisfazer.

Lema 4.1.1. Se (x,y,z)for um trio pitagórico primitivo ,x e y não podem ser ambos ímpares .

Demonstração (Redução ao absurdo). Suponhamos que x e y são ambos ímpares, digamos x=2a+1 e y=2b+1, então $x^2 + y^2 \equiv 2(\mathrm{mod}\,4)$. Por outro lado, como $x^2 e y^2$ também são ímpares, z^2 é par (soma de dois números ímpares é sempre par) pelo que também z é par (soma de dois números ímpares é sempre par) pelo que também z é par, digamos z=2c.Entao $z^2 = 4c^2$, isto é $z^2 \equiv 0(\mathrm{mod}\,4)$ o que é uma contradição com a hipótese, uma vez que estamos a supor que $X^2 + Y^2 = Z^2$.

Assim dos dois números x e y, pelo menos um é par.

Sem perda de generalidade supomos que é o y (se fosse x o raciocínio era análogo).

Corolário do lema 4.2.1. Se (x,y,z) for um trio pitagórico primitivo com y par ,x e z têm que ser ímpares

Demonstração . Se y é par então x tem que ser ímpar, porque se não 2 era um divisor comum de x, y e z. Sendo x ímpar, z também tem que ser ímpar, porque $X^2 + Y^2 = Z^2$

Lema 4.1.2. Se (x, y, z) for um trio pitagórico primitivo com y par tem-se (z+x, z-x) =2

Demonstração . É claro que z + x e z -x são ambos números pares pelo que 2| (z+x, z-x).

Seja (z+x, z-x) $\equiv 2d$.

Então 2d| (z +x) e 2d| (z-x). Daqui tira-se, por um lado que 2d divide a soma e a diferença de (z +x) e (z-x), isso é, 2d|2z e 2d|2x, donde d|z e d|x.

Por outro lado, multiplicando membro a membro as duas relações de divisibilidade, obtemos:

$4d^2 \mid (z+x)(z-x)$, isto é $4d^2 \mid z^2 - x^2$ ou seja $4d^2 \mid y^2$, donde $2d \mid y$ e portanto d|y.

Como d|x, d|y, d|z e x, y, z são primos entre si d tem que ser igual a 1.

Desta proposição concluímos que z+x=2h e z-x=2k com (h, k)=1. Segue-se que

$y^2 = z^2 - x^2 = (z+x)(z-x) = 4hk$

Mas y é par, digamos y =2s.Logo, tem-se $4s^2 = 4hk$, donde $s^2 = hk$, isto é, hk é um quadrado perfeito. Como h e k são primos entre si, o facto de o seu produto ser um quadrado perfeito implica que cada um deles seja também um quadrado perfeito.

Tem-se assim $h = a^2 e k = b^2$ com a e b números naturais primos entre si.

Em resumo tem-se:

$$\begin{cases} z+x = 2a^2 \\ z-x = 2b^2 \\ y^2 = 4a^2b^2 \end{cases} \Leftrightarrow \begin{cases} x = a^2 - b^2 \\ y = 2ab \\ z = a^2 + b^2 \end{cases}$$

Note-se que evidentemente, se tem a> b, e que a e b têm que ter paridades diferentes (se não, x e z não seriam ímpares)

Demonstramos assim o seguinte:

Teorema4.1.1. Se (x, y, z) for um trio pitagórico primitivo com y par então existem dois números naturais a e b primos entre si, de paridades diferentes e com a> b, tais que:

$x = a^2 - b^2$; $y = 2ab$; $z = a^2 + b^2$

Reciprocamente, é imediato que três números x, y e z desta forma constituem um trio pitagórico com y par, e podemos também ver que se trata de um trio pitagórico primitivo.

Descrevemos assim todos assim todos os possíveis trios pitagóricos primitivos (x, y, z) com y par.

Exemplos:

Tomando a=2 e b=1,obtemos o trio pitagórico (3,4,5)

Tomando a=4 e b=1,obtemos o trio pitagórico (15,8,17)

Tomando a=2 e b=2 obtemos o trio pitagórico (5,12,13)

4.2- MÉTODO GEOMÉTRICO DE RESOLUÇÃO DE EQUAÇÕES DO TIPO:

$$X^2 + Y^2 = Z^2 \qquad (1)$$

Consideremos agora o mesmo problema mas do ponto de vista geométrico:

É claro que x=y=z=0 é uma solução de (1).

Daqui em diante tomaremos z≠0 para todas as outras soluções de (1), obtemos:

$$x^2 + y^2 = 1$$

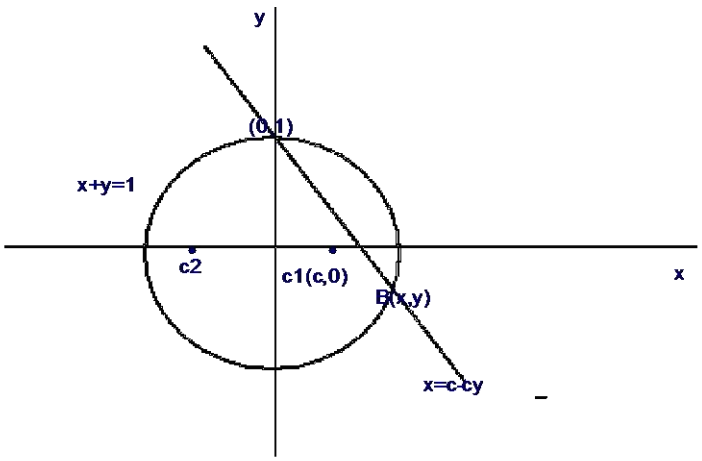
$$onde \;\; x = \frac{X}{Z} \;\; e \;\; y = \frac{Y}{Z} \qquad (2)$$

(2) é uma circunferência S de raio 1 e centro em (0,0)

O problema inicial reduziu-se ao problema seguinte:

Encontrar todos os pontos dessa circunferência que têm coordenadas racionais

Acontece, que existem tantos pontos com coordenadas racionais «pontos racionais» da circunferência (2), quanto «pontos racionais» na recta real



Alguns dos pontos é fácil de encontrar $(\pm 1,0),(0,\pm 1)$ escolhemos por exemplo, A= (0,1)

Tracemos por A diferentes (todos os possíveis) rectas (além da horizontal) que intersectam a circunferência dada em mais de que um ponto, digamos l: B (x, y)≠A (0,1), l intersecta também, o eixo de abcissas num ponto C= (c,0),com $x,y \in Q$

Desse modo, pondo em correspondência a cada ponto B um ponto C, obtemos uma bijecçao entre os pontos da circunferência s (além de A) e pontos da recta y=0

Isso é o sentido geométrico desse problema

4.3-RESOLUÇÃO ALGÉBRICA

Realmente essa bijecçao preserva a ´´racionalidade`` de um ponto.

Teorema 4.3.1. Um ponto B tem coordenadas racionais se e só se um número c é racional.

Demonstração . Uma recta l que passa por A e C se determina por x=c-cy

Logo $(c-cy)^2+y^2=1 ou (c^2-1)y^2-2c^2y+c^2-1=0$ donde y=1 (o que corresponde ao ponto A) ou $y=\frac{c^2-1}{c^2+1}\, e\, x=c-cy=\frac{2c}{c^2+1}$

Se $c \in Q$ então x, $y \in Q$, também

O recíproco obtém – se das afirmações:

Afirmação 4.3.1:Se as coordenadas de dois pontos são racionais, então a equação da recta que passa por eles tem coeficientes racionais.

Demonstração. Sejam os pontos A e B de coordenadas $A=(a_1,a_2)\, e\, B=(b_1,b_2)$.

A equação de recta l que passa pelos dois pontos A e B pode ser escrita sob a forma :

$$l:\frac{y-a_2}{x-a_1}=\frac{b_1-a_2}{b_1-a_1}=k\in Q$$

onde $a_i, b_i \in Q$

Donde segue

$$y - a_2 = \frac{b_1 - a_2}{b_1 - a_1}(x - a_1)$$

$$y - a_2 = \frac{b_1 - a_2}{b_1 - a_1}x - \frac{b_1 - a_2}{b_1 - a_1}a_1$$

$$y - a_2 = kx - ka_1$$

$$y = kx + (a_2 - ka_1)$$

$$com\ (a_2 - ka_1) \in Q$$

O que confirma a afirmação.

Afirmação 4.3.2. Se duas rectas se determinam pelas equações com coeficientes racionais então o ponto da sua intersecção (se existir) tem coordenadas racionais.

Demonstração. Sejam as rectas $l_1\ e\ l_2$ se determinam pelas funções lineares:

$y = k_1x + a_1$ e $y = k_2x + a_2$,respectivamente ,onde $k_1, k_2, a_1, a_2 \in Q$.

Então, encontrar o ponto da sua intersecção significa resolver o sistema:

$$\begin{cases} y = k_1x + a_1 \\ y = k_2x + a_2 \end{cases} \quad , k_1, k_2, a_1, a_2 \in Q$$

$$\Rightarrow (k_1 - k_2)x + (a_1 - a_2) = 0$$

$$\Rightarrow x = \frac{a_2 - a_1}{k_1 - k_2} \in Q$$

e

$$y = \frac{k_1(a_2 - a_1)}{k_1 - k_2} + a_1 = \frac{k_1a_2 - k_1a_1 + k_1a_1 - a_1k_2}{k_1 - k_2} = \frac{k_1a_2 - k_2a_1}{k_1 - k_2} \in Q$$

Seja $c = \frac{m}{n}(m, n \in Zen \neq 0).$ Então $x = \frac{2mn}{m^2 + n^2}, y = \frac{m^2 - n^2}{m^2 + n^2}$

Lembremos que o nosso objectivo é encontrar todas as soluções ´´inteiras`` da equação (1). Temos:

$$\frac{X}{Z} = \frac{2mn}{m^2 + n^2}, \frac{Y}{Z} = \frac{m^2 - n^2}{m^2 + n^2}, onde\ m^2 + n^2 \neq 0$$

As fracções $\frac{X}{Z}, \frac{Y}{Z}$ são irredutíveis, pois X, Y, Z são primos em pares.

Se soubéssemos que as fracções $\frac{2mn}{m^2+n^2}, \frac{m^2-n^2}{m^2+n^2}$ também são irredutíveis tomaríamos

X=2mn,Y$= m^2-n^2, Z = m^2+n^2$

Mas por exemplo, para m=5,n=2 ambas as fracções são redutíveis

Além disso, elas podem ser redutíveis só por 2.Com efeito, consideremos a

fracção $\frac{X}{Z} = \frac{2mn}{m^2+n^2}$.

Seja p (p≠2) número primo que é divisor de 2mn,isto é p|2mn.Se p|m então p não divide

n pois $\frac{m}{n}$ é irredutível.

Logo p não divide $(m^2+n^2) e \frac{2mn}{m^2+n^2}$ pode ser reduzido só por 2, caso m, n fossem

ímpares

Consideremos agora a fracção $\frac{m^2-n^2}{m^2+n^2}$

Se p $|(m^2-n^2)$e p$|(m^2+n^2)$ então p|2m^2 e p|2n.Mas (m,n)=1,logo p=2 e m,n são

ímpares .

Portanto, as soluções inteiras positivas primas em pares de (1) são:

- Para m> n> 0 e (m, n)=1 ,m,n-ímpares

$$X=mn,\ Y = \frac{m^2-n^2}{2}, Z = \frac{m^2+n^2}{2} \qquad (3)$$

- Para m> n> 0e (m, n)=1, onde pelo menos um dos números m, n é par

$$X=2mn,\ Y= m^2-n^2 \quad , Z = m^2+n^2 \qquad (4)$$

Quaisquer outras soluções de (1) obtêm-se de (3) ou (4) por multiplicação por um número natural.

É fácil ver que (3) e (4) coincidem, pois se

X=pq, $Y=\frac{p^2-q^2}{2}$, $Z=\frac{p^2+q^2}{2}$ soluções obtidas segundo a fórmula (3) (os números p e q ambos são impares e primos entre si), então a mesma solução se obtém de (4) tomando $m=\frac{p+q}{2}$, $n=\frac{p-q}{2}$, isto é

$$X=2\frac{p+q}{2}.\frac{p-q}{2}=\frac{2}{4}(p^2-q^2)=\frac{p^2-q^2}{2}$$

$$Y=\left(\frac{p+q}{2}\right)^2-\left(\frac{p-q}{2}\right)^2=p.q$$

$$Z=\left(\frac{p+q}{2}\right)^2+\left(\frac{p-q}{2}\right)^2=\frac{p^2+q^2}{2}$$

(verifique que (m, n)=1 e um dos números m ou n é par) e X, Y permutam.

Analogamente, qualquer solução da forma (4) pode ser escrita sob a forma (3).

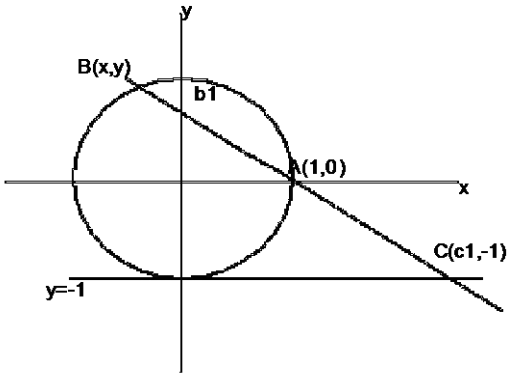
Desse modo podemos concluir que todos as soluções inteiras positivas de (1) se descrevem pelas formulas (4) até uma permutação de X e Y e multiplicação de X, Y, Z por um número natural.

Existe mais uma forma de escrever todos as soluções de (1)

X=2.m.n.r, $Y=(m^2-n^2)r$, $Z=\left(m^2+n^2\right)r$ (3´-4´)

onde m,n $\in$ Z, r-um número racional convenientemente escolhido ,isto é, tal que x,y,z inteiros.

Problema: Qual será conclusão se na qualidade do ponto A se toma (1,0) e consideram-se pontos de intersecção de rectas traçadas por esse ponto com recta y=-1 (e não com o eixo de abcissas)



Sentido geométrico:

Seja A (1,0), tracemos por A diferentes (todos possíveis) rectas (além da vertical) que intersectam a circunferência dada em mais um ponto digamos B= (x, y)≠A (1,0) l intersecta, também, a recta y=-1 num ponto C (c_1, -1).

Desse modo, pondo em correspondência a cada ponto B um ponto C, obtemos uma bijecçao entre os pontos da circunferência S (além de A) e pontos da recta y=-1

Sentido aritmético

$$l: x+\frac{y}{b_1}=1$$

$$l: x=1-\frac{y}{b_1} \quad \log o\left(1-\frac{1}{b_1}y\right)^2+y^2=1$$

$$\Leftrightarrow 1-\frac{2}{b_1}y+\frac{1}{b_1^{\,2}}y^2+y^2=1$$

$$\Leftrightarrow \left(\frac{1}{b_1^{\,2}}+1\right)y^2-\frac{2}{b_1}y=0$$

$$\Leftrightarrow \left(1+b_1^{\,2}\right)y^2-2b_1y=0$$

Donde y=0 (o que corresponde ao ponto A) ou $y=\frac{2b_1}{1+b_1^{\,2}} \quad e\ x=\frac{b_1^{\,2}-1}{b_1^{\,2}+1}$

Se $b_1 \in Q$ então $x, y \in Q$ também

Também se pode resolver a equação $x^2+y^2=z^2$ de uma outra forma (sem ter que recorrer à interpretação geométrica), contudo a solução é a mesma.

Teorema 4.3.1. As soluções (x, y, z) da equação $x^2+y^2=z^2$ com x, y, z inteiros não nulos são dados por:

$$(x,y,z)=(2.m.n.r,(m^2-n^2)r,(m^2+n^2)r)ou$$
$$(x,y,z)=((m^2-n^2)r,2.m.n.r,(m^2-n^2)r)$$

onde r,m,n são inteiros não nulos ,com m≠n,(m,n)=1 e m,n de paridades distintas .

Vejamos como o **teorema 4.3.1** pode ajudar na resolução de outros problemas por exemplo determinar as soluções inteiras não nulos da equação

$$x^2+y^2=2z^2 com\ x\neq y$$

É fácil ver que x e y devem ser da mesma paridade, pois caso contrario $x^2 + y^2$ seria um número ímpar. Assim, existem inteiros a e b tais que x=a+b, y=a-b

Basta tomarmos $a = \frac{1}{2}(x+y)\ e\ b = \frac{1}{2}(x-y)$, notando que x+y e x-y, são números pares.

Substituindo as expressões acima para x e y na equação original, concluindo que

$$x^2 + y^2 = 2z^2 = a^2 + b^2 = z^2$$

Mas essa ultima é a nossa já conhecida equação de Pitágoras. Então de acordo com o **teorema4.3.1**, podemos escrever

$(a,b,z) = ((2.m.n,(m^2 - n^2)r,(m^2 + n^2)r)\ ou$
$(a,b,z) = ((m^2 - n^2)r,2.m.n.r,(m^2 + n^2)r)$

onde r,m,n são inteiros não nulos com m≠n ,(m,n)=1 e m,n de paridades distintas .

Segue daí que as soluções (x, y, z)da nossa equação são de um dos tipos abaixo, onde r, m, n satisfazem as mesmas condições do **teorema 4.3.1**

$(x,y,z) = ((2.m.n + (m^2 - n^2)r, 2mnr - (m^2 - n^2)r, (m^2 + n^2)r)\ \ ou$
$(x,y,z) = ((m^2 - n^2)r + 2.m.n.r, (m^2 - n^2)r - 2mnr, (m^2 + n^2)r)$

Exemplo:

Descrever soluções em z da equação:

$$X^2 + 2Y^2 = 3Z^2 \qquad (5)$$

Notemos que a única solução para z=0 é x=y=z=0

Consideremos os casos quando z≠0 obtêm:

$$x^2 + 2y^2 = 3 \qquad (6)$$

onde $x = \frac{X}{Z}$ $, y = \frac{Y}{Z}$ -números racionais

A equação (6) define uma elipse de semieixos $\sqrt{3}$ e $\frac{1}{2}\sqrt{6}$ com centro (0,0). É fácil encontrar um ponto “racional “ nessa elipse como tal é A= (1,1)

Como no problema sobre trios pitagóricos, existe uma bijecçao entre os pontos da elipse (além de (-1,1)) e pontos da recta y=0,isto é, existe tantos pontos "racionais " na elipse quantos pontos "racionais" na recta.

A equação da recta l que passa por A= (1,1) e (c, 0) é l: x=c+ (1-c) y então

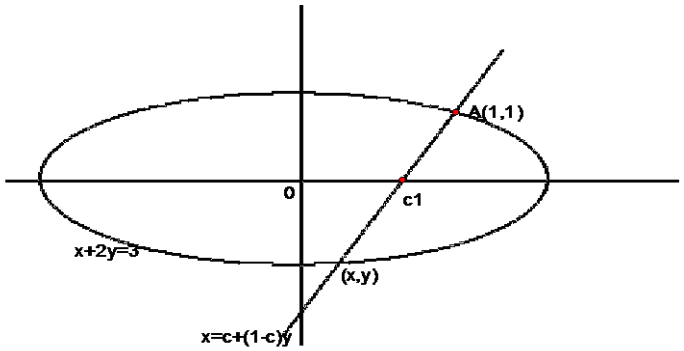
$(c+(1-c)y)^2+2y^2=3$

Uma raiz conhecida é 1

Utilizando o teorema de Viett encontramos a segunda raiz

$$y=\frac{c^2-3}{c^2-2c+3}\log o, x=c+(1-c)y=\frac{-c^2+6c-3}{c^2-2c+3}$$

(**obs**: para c=3 temos: x=1, y=1-é o ponto de tangencia mas não obtemos o ponto (-1,1))



Tendo em conta a **afirmação 4.3.1**,concluímos que todas as soluções racionais de (6) se descrevem pelas fórmulas:

$x=\frac{c^2+6c-3}{c^2-2c+3}$, $y=\frac{c^2-3}{c^2-2c+3}$ onde $c\in Q$ (além de x=-1,y=1 que corresponde a recta horizontal)e as soluções inteiras de (5)-pelas formulas

$X=(-m^2+6mn-3n^2)r,\quad Y=(m^2-3n^2)r,\quad Z=(m^2-2mn+3n^2)r$

Nota: Para outra escolha de A, pertencente a elipse, as formulas finais podem ser outras, mas, é claro, que o conjunto das soluções por elas descrito é o mesmo.

4.4-NUMEROS CONGRUENTES

As formulas (3´-4´) dão todas as soluções racionais de

$X^2 + Y^2 = Z^2$

Quando r toma quaisquer valores racionais.

Definição 4.4.1. Ao número racional **s** chama-se congruente se existe um triângulo rectângulo de área s com lados que são números racionais.

Como determinar os números congruentes?

A descrição de todos os números congruentes baseia-se em teoremas e hipóteses da geometria algébrica, é complexo.Mas para alguns números existe resposta é positiva. Por exemplo, para triângulo rectângulo de lados 3,4,5 temos

$s = \frac{1}{2}.3.4 = 6,$ logo ,6 é um numero congruente.

5 é também um número congruente ,pois 5 é a área do triangulo rectângulo de lodos $\frac{3}{2};\frac{20}{3};\frac{41}{6}$,o que é fácil de verificar ,mas demonstrar não é .

.

Teorema 4.4.1. (Fermat) -O número 1 não é congruente.

Demonstração. Suponhamos o contrário, isto é, 1 é um número congruente.
Isso significa que existe um triângulo rectângulo com lados de comprimentos-números inteiros a, b, x (x – comprimento da hipotenusa), cuja área é igual a $\frac{1}{2}a.b = y^2, \quad y \in Z$

(é claro, que podemos escolher a e b de tal modo que só um deles fosse par).

Transformemos a expressão $x^4 - 16y^4$, obtemos:

$$x^4 - 16y^4 = \left(x^2 - 4y^2\right)\left(x^2 + 4y^2\right) = \left(x^2 - 2ab\right)\left(x^2 + 2ab\right)$$
$$= \left(a^2 + b^2 - 2ab\right)\left(a^2 + b^2 + 2ab\right) = \left(a - b\right)^2\left(a + b\right)^2$$

Se 1 é um número congruente, então a equação $x^4 - \left(2y\right)^4 = u^2$ tem solução em Z^+ (u é impar). Escolhemos entre todas as soluções não nulas com u impar tal que |u| é mínimo. Seja (x_0, y_0, u_0) tal solução. Os números x_0, y_0, u_0 são primos em pares, pois se

quaisquer dois deles tivessem um divisor primo comum p, o terceiro número devia dividir-se por p (alem disso, u_0 devia dividir por p^2) e para a solução $\left(\frac{x_0}{p}, \frac{y_0}{p}, \frac{u_0}{p}\right)$ o valor de |u| é menor.

Aplicando fórmulas (4) para a equação $x_0^4 = (2y_0)^4 + u_0^2$, obtemos

$x_0^2 = m^2 + n^2, (2y_0)^2 = 2mn$(no caso os números $x_0^2, (2y_0)^2 \; e \; u_0$ primos em pares e $(2y_0)^2$ é ímpar), onde m, n-primos entre si, um deles, digamos n, é par.

De $(2y_0)^2$=2mn segue que $m = m_1^2, n = 2n_1^2$.

$De \; x_0^2 = m^2 + n^2 \; segue \; que \; x_0 = m_2^2 + n_2^2,$
$n = 2m_2 n_2 = 2n_1^2,$
$m = m_2^2 - n_2^2 = m_1^2, onde \; m_2, n_2 - primos \; entre \; si, n_2 - par$

Finalmente, $m_2 = m_3^2, n_2 = n_3^2, m_3^4 - n_3^4 = m_1^2$ e assim como n_3 é par, temos

$\left(m_3, \frac{n_3}{2}, m_1\right)$ – solução de $x^4 - (2y)^4 = u^2 em \quad Z$ com |u| menor que $|u_0|$:

$|u_0| = |m^2 - n^2| \geq 2m - 1 = 2m_1^2 - 1 e \; |m_1| \leq \sqrt{\frac{|u_0|+1}{2}} < |u_0|$

Para $|u_0| > 1$.Caso $|u_0| = 1$trivial

OBS: O modo utilizado nessa demonstração chama se método descida infinita e tem vasta aplicação na resolução de problemas da teoria de números

O teorema dos números congruentes tem origem na Grécia Antiga. A resposta foi formulada só no século XX.

Os números congruentes de 1 até 100 são:

5;6;7;13;13;15;21;22;23;29;30;31;34;38;39;41;46;53;55;65;69;70;71;77;78;85;86;87;
93;94;95.

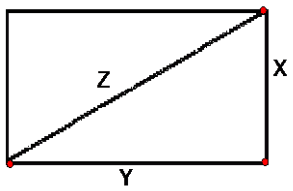
A tabela seguinte apresenta os respectivos triângulos por eles formados:

7	$\frac{24}{5},\frac{35}{12},\frac{337}{69}$	34	$\frac{136}{16},\frac{15}{2},\frac{353}{90}$	70	$15,\frac{28}{3},\frac{53}{3}$
13	$\frac{780}{328},\frac{323}{30},\frac{106921}{9690}$	38	$\frac{5301}{425},\frac{1700}{279},\frac{1646021}{118576}$	71	$\frac{30317}{660},\frac{1320}{427},\frac{12974641}{281820}$
14	$\frac{21}{2},\frac{8}{3},\frac{65}{6}$	39	$\frac{312}{10},\frac{6}{2},\frac{318}{10}$	77	$\frac{525}{848},\frac{18656}{75},\frac{15820337}{63600}$
15	$\frac{15}{2},4,\frac{17}{2}$	41	$\frac{40}{3},\frac{123}{20},\frac{881}{60}$	78	$45,\frac{52}{15},\frac{677}{15}$
21	$12,\frac{7}{2},\frac{25}{2}$	46	$\frac{253}{42},\frac{168}{11},\frac{7585}{462}$	85	$\frac{77}{6},\frac{120}{77},\frac{8521}{462}$
22	$\frac{1540}{33},\frac{33}{35},\frac{53911}{105}$	53	$\frac{1472112483}{202332130},\frac{21447205780}{1472112483}$, $\frac{485049389732978596 1}{297855654284978790}$	86	$\frac{2193}{91},\frac{364}{51},\frac{116645}{4641}$
23	$\frac{41496}{3485},\frac{80155}{20748},\frac{9051416}{7230678}$			87	$\frac{3484}{1925},\frac{167475}{1742},\frac{322446497}{3353350}$
29	$\frac{52780}{99},\frac{99}{910},\frac{48029801}{90090}$	55	$\frac{117}{10},\frac{1100}{117},\frac{17561}{1170}$	93	$\frac{56203}{1330},\frac{7980}{1813},\frac{2090761}{49210}$
30	12,5,13	65	$12,\frac{65}{6},\frac{97}{6}$	94	$\frac{7728}{2057},\frac{96679}{1932},\frac{199428385}{3974124}$
31	$\frac{8897}{360},\frac{720}{287},\frac{2566561}{103320}$	69	$\frac{437}{104},\frac{624}{19},\frac{65425}{1976}$	95	$\frac{1443}{34},\frac{6460}{1443},\frac{2093801}{49062}$

4.5 BLOCOS PITAGÓRICOS

Os problemas sobre triângulos pitagóricos podem ser formulado de outra maneira.

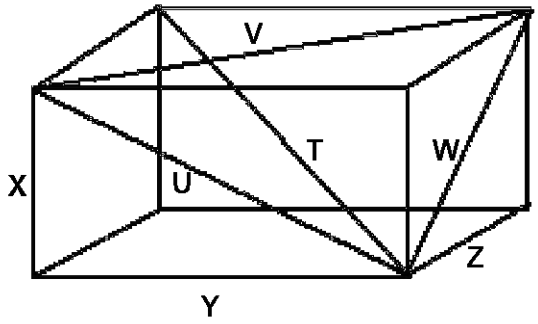
Definição 4.5.1. Ao rectângulo chama-se pitagórica se comprimentos dos seus lados X e Y, também sua diagonal Z são números inteiros



Nessa formulação o problema tem generalização:

Definição 4.5.2. Ao paralelepípedo rectangular chama-se bloco pitagórico se suas arestas X, Y, Z, diagonais das faces U,V,W e diagonal principal T são números inteiros.

Se T não é inteiro, ao bloco chama-se pitagórico fraco.



Exemplo:

X=44, Y=117, Z=240,

U=125, V=244, W=267

Formam um bloco pitagórico fraco.

Existem pelo menos um bloco pitagórico?

Como descrever todos os blocos pitagóricos fracos?

As respostas ainda não existem. Mas podemos pensar sobre:

a) Como interpretar os problemas na ´´linguagem de equações ``?

b) Descrever todos os paralelepípedos com X, Y, Z e T inteiros.

c) Verificar que $\forall n \in N, n \geq 2$ o bloco de arestas

$X = n^6 - 15n^4 + 15n^2 - 1,$

$Y = 6n^5 - 20n^3 + 6n,$

$Z = 8n^5 - 8n$

é pitagórico fraco.

Respostas (indicações)

a) Para um bloco pitagórico temos $\begin{cases} x^2+y^2=z^2, \\ y^2+z^2=v^2, \\ z^2+x^2=w^2, \\ x^2+y^2+z^2=t^2 \end{cases}$

Também, para um bloco pitagórico ´´fraco``temos: $\begin{cases} x^2+y^2=z^2, \\ y^2+z^2=v^2, \\ z^2+x^2=w^2, \end{cases}$

Dividindo todas as incógnitas por uma delas, por exemplo, por u, obtemos um sistema de 4 equações com 6 incógnitas (respectivamente, um sistema de 3 equações de 5 incógnitas). Os objectos geométricos correspondentes são superfícies algébricas que pertencem aos espaços n-dimencionais e têm um número finito dos pontos notáveis.

b) Descrever todos os paralelepípedos com inteiros x, y, z significa descrever todas as soluções inteiras da equação:

$X^2+Y^2+Z^2=T^2$

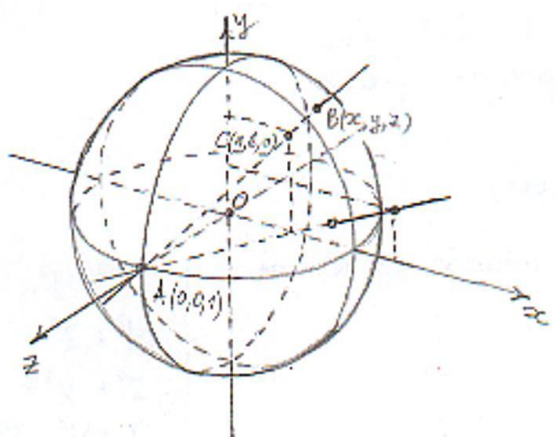
A única solução dessa equação com T=0 é X=Y=Z=0=T.

Para outras t≠0 e a equação pode ser representada sob a forma

$x^2+y^2+z^2=1,$

$onde\ x=\frac{X}{T}, y=\frac{Y}{T}, z=\frac{Z}{T}$

Essa equação determina uma esfera no espaço 3-dimencional (0xyz).



Escolhemos em esfera um ´´ponto racional`` A (0,01).

É fácil ver que qualquer recta, onde B (x, y, z)-um ponto racional, intersecta o plano Oxy num ´´ponto racional`` C (a, b, 0) e vice-versa, cada recta AC intersecta a esfera num ponto racional B. Desse modo, na esfera há tantos pontos racionais quanto no plano.

Os números x, y, z exprimem-se por a, b, do modo seguinte:

$$x = \frac{2a}{a^2+b^2+1}, y = \frac{2b}{a^2+b^2+1}, z = \frac{a^2+b^2-1}{a^2+b^2+1}$$

Tomando $a = \frac{k}{l}, b = \frac{m}{n}$, obtemos, finalmente:

$X = 2k\ln^2 r;$

$Y = 2l^2 mnr;$

$Z = \left(k^2n^2 + l^2m^2 - l^2n^2\right)r;$

$T = \left(k^2n^2 + l^2m^2 - l^2n^2\right)r,$

Onde $k, l, m, n \in Z, r \in Q \rightarrow$ convenientemente escolhido

Isto é, tal que X, Y, Z, T serão inteiros

c) Mostremos que $x^2+y^2, y^2+z^2, z^2+x^2$ são quadrados exactas dos polinómios com coeficientes inteiras.Deste modo, qualquer que seja n pertencente a Z os números u, v, w, pertencem a Z

Assim:

$$x^2+y^2=\left(n^6-15n^4+15n^2-1\right)^2+\left(6n^5-20n^3+6n\right)^2=\left(n^6+3n^4+3n^2+1\right)^2,$$

$$y^2+z^2=\left(6n^5-20n^3+6n\right)^2+\left(8n^5-8n\right)^2=\left(10n^5-12n^3+10n\right)^2,$$

$$z^2+x^2=\left(8n^5-8n\right)^2+\left(n^6-15n^4+15n^2-1\right)^2=\left(n^6+17n^4-17n^2-1\right)^2$$

donde

$$u=n^6+3n^4+3n^2+1$$

$$v=10n^5-12n^3+10n$$

$$w=n^6+17n^4-17n^2-1$$

V

EQUAÇÕES DE FERMAT

A equação $x^2 - Dy^2 = 1$ frequentemente utiliza-se sob o nome Pell, pois em obras de Euler apareceu sob este nome. Mas Pell não investigou essa equação. Euler, por engano, utilizou o nome de Pell para equação $x^2 - Dy^2 = 1$.

Fermat, o que tudo indica, foi o primeiro, quem descobriu o método de resolução da equação $x^2 - Dy^2 = 1$ e por isso, muitos matemáticos chamam a equação (indicada) mencionada sob o nome de Fermat.

Fermat sabia como demonstrar que essa equação tem um número infinito de soluções para $D \in Z^+$, diferente de um quadrado perfeito, mas não publicou a sua demonstração e propôs esse problema aos matemáticos Brauker e Vallice (ingleses)

Só Lagrange demonstrou que $\forall D \in Z^+$, diferente de um quadrado perfeito, $x^2 - Dy^2 = 1$tem soluções inteiras.

Consideremos a equação da forma

$$x^2 - Dy^2 = 1 \qquad (1)$$

Onde D é um numero inteiro positivo, definida sobre o anel dos números inteiros Z.

São possíveis duas situações:

-D é um quadrado perfeito, isto é, $D = B^2 com\ B \in Z$.

Neste caso (1) pode ser escrita do modo seguinte:

(x-By) (x+By) =1

Se tiver uma solução x_0, y_0 , como o produto de dois inteiros é 1 se e só se ambos são iguais a 1 ou a -1,deverá ter-se:

$x_0 - By_0 = 1\, e \quad x_0 + By_0 = 1$

$ou \quad x_0 - By_0 = -1\, e \quad x_0 + By_0 = -1$

É fácil de ver que, então, só existe a solução trivial $x_0 = \pm 1 \quad , y_0 = 0$

- D não é um quadrado perfeito, então (1) terá uma infinidade de soluções e $\sqrt{D}$ é irracional .

5.1-RESOLUÇÃO POR MEIO DE FRACÇÕES CONTÍNUAS INFINITAS

Teorema 5.1.1. Seja $D \in Z^+$ diferente de um quadrado perfeito e $x_0, y_0 (x_0 > 0, y_0 > 0)$ uma solução de (1), então $x_0\ e\ y_0$ são, respectivamente, um numerador e um denominador de uma fracção próxima a $\sqrt{D}$

Demonstração. $x_0^{\,2} - Dy_0^{\,2} = 1 \Rightarrow \dfrac{x_0}{y_0} > \sqrt{D} > 1$

Também $(x_0 - \sqrt{D}y_0)(x_0 + \sqrt{D}y_0) = 1 \Rightarrow \left|\dfrac{x_0}{y_0} - \sqrt{D}\right| = \dfrac{1}{y_0^{\,2}\left|\dfrac{x_0}{y_0} + \sqrt{D}\right|} < \dfrac{1}{2y_0^{\,2}},$

Isto, é segundo um **teorema** (Se para os inteiros a, b (a, b)=1, b> 0) se verifica a condição

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2},$$

então $\frac{a}{b}$ uma das fracções próximas a um número real α),

$\frac{x_0}{y_0} = \frac{p_s}{Q_s}$ uma das fracções próximas a $\sqrt{D}$ .Sendo que x_0, y_0 satisfazem a (1) e são

primos entre si, então de $\frac{x_0}{y_0} = \frac{P_s}{Q_s}$ segue que $x_0 = P_s$, $y_0 = Q_s$.

Sabendo que a decomposição de $\sqrt{D}$ em fracção contínua tem a forma

$$\sqrt{D} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 \ddots \quad \cfrac{1}{a_{k-1} + \cfrac{1}{2a_0} + \ldots}}}} \qquad (2)$$

(**Teorema** -seja D não é um quadrado perfeito, Q –um inteiro tal que $D > Q^2 > 0$,então

a decomposição de $\frac{\sqrt{D}}{Q}$ em fracção contínua infinita tem a forma :

$$\frac{\sqrt{D}}{Q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 \ddots \quad \cfrac{1}{a_{k-1} + \cfrac{1}{2a_0} + \ldots}}}}$$

)

Podemos demonstrar que as soluções de (1) são numeradores e denominadores de tais

fracções próximas $\frac{P_s}{Q_s}$ que têm índices s da forma $kn-1$

<u>Teorema 5.1.2.</u> Se $x_0, y_0 (x_0 > 0, y_0 > 0)$ é uma solução da equação (1), então

$x_0 = P_{kn-1}, y_0 = Q_{kn-1}$, *onde* $\frac{P_{kn-1}}{Q_{kn-1}}$ -fracção próxima a (2).

Demonstração . Do **teorema 3.1.1** segue que $x_0 = p_s, y_0 = Q_s$ onde $\frac{P_s}{Q_s}$ uma fracção próxima a $\alpha = \sqrt{D}$

α é a raiz da equação quadrática com coeficientes inteiros –(é a irracionalidade quadrática)

$$x^2 - D = 0 \qquad (3)$$

O quociente incompleto $\alpha_{s+1} = a_{s+1} + \frac{1}{a_{s+2} + \ldots}$

da decomposição de $\sqrt{D}$ em fracções contínuas é a raiz de uma equação do segundo grau:

$$A_{s+1}\alpha^2{}_{s+1} + B\alpha_{s+1} + c_{s+1} = 0 \qquad (4)$$

Com o mesmo discriminante que a equação (3)

(**teorema** –Se uma irracionalidade quadrática α se representa sob a forma

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{\alpha_n}}}}$$

onde todos os a_i inteiros positivos (i=1,2, …) e $a_0 \in Z$, então α_n também é uma irracionalidade quadrática com o mesmo discriminante que α).

Logo, tendo em conta que

$A_n = AP^2{}_{n-1} + BP_{n-1}Q_{n-1} + CQ^2{}_n$,

$B_n = 2AP_{n-1}.P_{n-2} + B(P_{n-1}Q_{n-2} + P_{n-2}Q_{n-1}) + 2CQ_{n-1}Q_{n-2}$,

$C_n = AP^2{}_{n-2} + BP_{n-2} + CQ^2{}_{n-2}$,

$para\ n = s+1, B = 0, C = -D, obtemos:$

$A_{s+1} = P^2{}_s - DQ^2{}_s = 1$,

$B_{s+1} = 2(P_sP_{s-1} - DQ_sQ_{s-1})$,

B_{s+1} é um número par que designemos por -2l.

Resolvendo (4) relativamente a α_{s+1} obtemos que

$$\alpha_{s+1} = l + \sqrt{D},$$

Isto é a decomposição de α_{s+1} em fracção contínua infinita deve ter o mesmo período que a decomposição (2) de $\sqrt{D}$ e só se distingue dessa por membro inicial. Isso só pode acontecer quando $l = a_0, s+1 = kn$, *isto e* $s = kn-1$.

Agora, falta esclarecer, quais das números P_{kn-1}, Q_{kn-1} são soluções de (1).

Teorema 5.1.2. Seja D-inteiro positivo que não é um quadrado perfeito, k-comprimento do período da decomposição de $\sqrt{D}$ em fracção contínua infinita. Todas as soluções inteiras de (1) se encontram, pondo:

$x = P_{kn-1}$ *e* $y = Q_{kn-1}$, *onde* $n \in N \setminus \{0\}$ *tal que* kn é par.

Demonstração . Já sabemos que todas as soluções inteiras positivas de (1) se encontram dentre pares da forma P_{kn-1}, Q_{kn-1}.

Só falta esclarecer, para que valores de n os números $x_0 = P_{kn-1}$, $y_0 = Q_{kn-1}$ satisfazem (1).

O quociente incompleto α_{kn} na decomposição (2) de $\sqrt{D}$ tem a forma:

$$\alpha_{kn} = 2a_0 + \cfrac{1}{a_1 + \cfrac{1}{\cfrac{1}{a_{k-1} + \ldots}}} = a_0 + \sqrt{D} \qquad (5)$$

Sabendo (da teoria de fracções continuas infinitas) que:

$$\sqrt{D} = \frac{P_{kn-1}\alpha_{kn} + P_{kn-2}}{Q_{kn-1}\alpha_{kn} + Q_{kn-2}}.$$

Donde, utilizando (5), obtemos:

$$DQ_{kn-1} + (a_0 Q_{kn-1} + Q_{kn-2})\sqrt{D} = (a_0 P_{kn-1} + P_{kn-2}) + P_{kn-1}\sqrt{D} \qquad (6)$$

Tendo em conta que $\sqrt{D}$ é um numero irracional, de (6) segue que:

$$P_{kn-1} = a_0 Q_{kn-1} + Q_{kn-2}$$
$$DQ_{kn-1} = a_0 P_{kn-1} + P_{kn-2},$$

Donde, multiplicando a primeira igualdade por P_{kn-1} e a segunda por Q_{kn-1}, e subtraindo-as obtemos:

$$P^2_{kn-1} - DQ^2_{kn-1} = P_{kn-1}Q_{kn-2} - P_{kn-2}Q_{kn-1} = (-1)^{kn}$$

Portanto, o par P_{kn-1}, Q_{kn-1} será uma solução de (1) se e só se $(-1)^{kn}$ =1, isto é, para kn – números pares .

Os mínimos positivos inteiros x_0, y_0 que satisfazem a (1) são:

$$x_0 = P_{k-1}, y_0 = Q_{k-1}, se\ k - par$$
$$x_0 = P_{2k-1}, y_0 = Q_{2k-1}, se\ k - impar$$

Sendo (x_0, y_0) a solução mínima e (x, y uma solução qualquer teremos, para um certo n

$x + \sqrt{D}y = (x_0 + \sqrt{D}y_0)^n$ e também

$x - \sqrt{D}y = (x_0 - \sqrt{D}y_0)^n$

Exemplo:

Encontrar os números inteiros positivos mínimos que satisfazem ás equações:

$x^2 - 11y^2 = 1$

D=11

A decomposição de $\sqrt{11}$ em fracções contínuas infinitas tem a forma:

$$\sqrt{11} = 3 + \cfrac{1}{6 + \cfrac{1}{6 + \cfrac{1}{\ddots}}}$$

Sendo assim K=6 que é um número par logo:

$x_0 = p_{k-1}, \quad y_0 = Q_{k-1}$

Então

$x_0 = P_5 \quad , y_0 = Q_5$

$x_0 = 4181 \quad , y_0 = 1292$

A solução geral é dada por:

$$x+\sqrt{11}y=(4181+\sqrt{11}.1292)^{n}$$

$$x-\sqrt{11}y=(4181-\sqrt{11}.1292)^{n}$$

OBS: De modo análogo, podemos resolver equação

$x^2-Dy^2=-1.$

Os **teoremas 5.1.1 e5.1.2** aplicam-se sem alterações

O **teorema 3.1.3** no lugar da condição´´ kn par´´, devemos exigir que ´´2 não divide kn``, desse modo para os valores pares de k, a equação $x^2-Dy^2=-1$não terá soluções, pois se fosse 2|kn teriam $(-1)^{kn}=1$e não $(-1)^{kn}=-1.$

Consideremos agora a equação mais geral:

$$x^2-Dy^2=m, \qquad (7)$$

onde m é inteiro qualquer.

Lema 5.1.1. Seja D um inteiro positivo que não seja um quadrado perfeito. Existe um inteiro m para o qual a equação $x^2-Dy^2=m$ admite infinitas soluções inteiras positivas.

Demonstração . Desenvolvemos o número α=$\sqrt{D}$ em facção contínua infinita. R_i, P_i, Q_i (reduzida, numerador e denominador das fracções próximas á fracção continua α).

Consideremos o binómio x^2-Dy^2 e substituímos x por P_{2n-1} e y por Q_{2n-1}.Designando por Z_{2n-1} o resultado teremos

$$Z_{2n-1}=P^2{}_{2n-1}-DQ^2{}_{2n-1}=\left(P_{2n-1}-\sqrt{D}Q_{2n-1}\right)\left(P_{2n-1}+\sqrt{D}Q_{2n-1}\right) \qquad (8)$$

Utilizando o **teorema 2.1.11**dos conceitos preliminares e recordando que com D positivo é $P_i>0, Q_i>0$, podemos escrever:

$$0<P_{2n-1}+\sqrt{D}Q_{2n-1}=2\sqrt{D}Q_{2n-1}+P_{2n-1}-\sqrt{D}Q_{2n-1}<$$

$$<2\sqrt{D}Q_{2n-1}+\frac{1}{Q_{2n}} \qquad (9)$$

Ainda segundo o mesmo teorema temos

$$0< P_{2n-1} - \sqrt{D}Q_{2n-1} < \frac{1}{Q_{2n}} \qquad (10)$$

Substituído (2) e (3) em (1) vem

$$0< Z_{2n-1} < \frac{1}{Q_{2n}}\left(2\sqrt{D}Q_{2n-1} + \frac{1}{Q_{2n}} \right) < 2\sqrt{D} + 1$$

Se em Z= $x^2 - Dy^2$ substituímos x por P_{2n-1} e y por Q_{2n-1}, qualquer que seja n, Z toma o valor Z_{2n-1} inteiro positivo nunca superior ao numero fixo $2\sqrt{D}+1$.

Como $\sqrt{D}$ é irracional a respectiva fracção contínua é infinita. Por conseguinte há uma infinidade de pares P_{2n-1}, Q_{2n-1}.

Entre os números inteiros e positivos $Z_1, Z_3, ...Z_{2n-1}, ...$ só pode haver uma quantidade finita deles distintos dois a dois uma vez que não ultrapassam $2\sqrt{D}+1$.

Portanto de entre os pares $(P_1, Q_1), (P_3, Q_3), ..., (P_{2n-1}, Q_{2n-1}), ...$ há uma infinidade que torna $x^2 - Dy^2$ igual a um mesmo inteiro m com $1 \le m < 2\sqrt{D}+1$

Ficou demonstrado a afirmação do lema

OBS: designemos por (u_n, v_n), n=1,2, …os infinitos pares de inteiros que satisfazem

$$u_n{}^2 + Dv_n{}^2 = m$$

Notemos que a sucessão dos pares (u_i, v_i) pode ser escolhida como parte da sucessão dos pares de numeradores e denominadores das reduzidas impares do número $\sqrt{D}$.

5.2- OUTRO OLHAR SOBRE O MESMO PROBLEMA

Teorema 5.2.1. Seja D um inteiro positivo que não seja um quadrado perfeito. A equação $x^2 - Dy^2 = 1$ admite infinitas soluções em inteiros positivos x, y. Ademais, existe uma solução em inteiros positivos x_1, y_1 tal que todas as demais soluções dessa equação são da forma $x_n + y_n\sqrt{D} = \left(x_1 + y_1\sqrt{D}\right)^n \quad \left(n \in N \setminus \{0\}\right)$

e $x_n - y_n\sqrt{D} = \left(x_1 - y_1\sqrt{D}\right)^n$

Também

$$x_n = \frac{1}{2}\left[\left(x_1 + \sqrt{D}y_1\right)^n + \left(x_1 - \sqrt{D}y_1\right)^n\right]$$

$$y_n = \frac{1}{2\sqrt{D}}\left[\left(x_1 + \sqrt{D}y_1\right)^n - \left(x_1 - \sqrt{D}y_1\right)^n\right]$$

Demonstração. Admitamos por enquanto que a nossa equação tenha uma solução em inteiros positivos x, y.Dentre todas essas soluções escolha aquela x_1, y_1 tal que $\alpha = x_1 + y_1\sqrt{D}$ seja o menor possível.

Dado um natural n, sabemos que existem inteiros positivos x_n, y_n tais que $\left(x_1 - y_1\sqrt{D}\right)^n = x_n + y_n\sqrt{D}$. Daí sabemos que

$\left(x_1 - y_1\sqrt{D}\right)^n = x_n - y_n\sqrt{D}$ e assim

$$1 = \left(x_1^2 - Dy_1^2\right)^n = \left[\left(x_1 + \sqrt{D}y_1\right)^n\left(x_1 - \sqrt{D}y_1\right)^n\right]$$

$$\left(x_n + y_n\sqrt{D}\right)\left(x_n - y_n\sqrt{D}\right) = x_n^2 - y_n^2$$

Então todos os pares (x_n, y_n) são soluções da equação.

Seja agora (x, y) uma solução qualquer em inteiros positivos. Para terminar, basta mostrar que existe um natural n tal que $x + y\sqrt{D} = \alpha^n$.

Suponha o contrário. Então existe um natural n tal que

$\alpha^n < x + y\sqrt{D} < \alpha^{n+1}$. Daí vem que $1 < \alpha^{-n}\left(x + y\sqrt{D}\right) < \alpha$

Mas $\alpha^{-n}(x+y\sqrt{D})=\left(x_1+y_1\sqrt{D}\right)^{-n}(x+y\sqrt{D})=\left(x_n+y_n\sqrt{D}\right)^{-1}\left(x+y\sqrt{D}\right)$

$=\left(x_n-y_n\sqrt{D}\right)\left(x+y\sqrt{D}\right)=\left(x.x_n-Dy.y_n\right)+\left(x_ny-y_nx\right)\sqrt{D}$

E ocorre que

$$\left(xx_n-Dyy_n\right)^2-D\left(x_ny-y_nx\right)^2=x_n{}^2\left(x^2-Dy^2\right)+y_n{}^2\left(Dy^2-x^2\right)=x_n{}^2-Dy_n{}^2=1$$

$\alpha^{-n}\left(x+y\sqrt{D}\right)=\left(xx_n-Dyy_n,x_ny-y_nx\right)$ também é solução .Como 1

$<\alpha^{-n}\left(x+y\sqrt{D}\right)<\alpha$, basta mostrarmos que $xx_n-Dyy_n>0$ e $x_ny-y_nx>0$ para

chegarmos a mesma contradição.Sejam $a=xx_n-Dyy_n$ e $b=x_ny-y_nx$.

Temos que $a+b\sqrt{D}>0$ e $a^2-Db^2=1$ donde $a-b\sqrt{D}=(a+b\sqrt{D})^{-1}>0.$

Então, $2a=(a+b\sqrt{D})+\left(a-b\sqrt{D}\right)>0$

Por outro lado,

$a+b\sqrt{D}>1$ implica $a-b\sqrt{D}=\left(a+b\sqrt{D}\right)^{-1}<1$,e daí

$b\sqrt{D}>a-1\geq 0$.Logo b> 0

Para terminar, basta mostrarmos que a equação $x^2-Dy^2=1$ admite uma solução.

Tome-se, de, acordo com o ***lema 5.2.2***,um inteiro (não nulo) m tal que $x^2-Dy^2=m$ admita uma infinidade de soluções. Podemos escolher duas dessas soluções $(x_1,y_1),(x_2,y_2)$,tais que $|x_1|\neq|x_2|mas\ x_1\equiv x_2\pmod m\ e\ y_1\equiv y_2\pmod m$.

Então

$$\left(x_1+y_1\sqrt{D}\right)\left(x_2-y_2\sqrt{D}\right)=\left(x_1x_2-Dy_1y_2\right)+\left(x_2y_1-x_1y_2\right)\sqrt{D}\quad(*)$$

$$Mas\ x_1x_2-Dy_1y_2\equiv x_1{}^2-Dy_1{}^2\equiv 0\pmod m\ e\ x_2y_1\equiv x_1y_2\pmod m$$

Donde existem inteiros u e v tais que:

$x_1x_2-Dy_1y_2=mu, x_2y_1-x_1y_2=mv$

Segue de $(*)$ que $\left(x_1+y_1\sqrt{D}\right)\left(x_2-y_2\sqrt{D}\right)=m\left(u+v\sqrt{D}\right)$ e daí

$$\left(x_1-y_1\sqrt{D}\right)\left(x_2+y_2\sqrt{D}\right)=m\left(u-v\sqrt{D}\right)$$

Multiplicando ordenadamente essas duas igualdades chegamos a

$m^2=(x_1{}^2-Dy_1{}^2)\left(x_2{}^2-Dy_2{}^2\right)=m^2(u^2-Dv^2)$ ou seja $u^2-Dv^2=1$.

Resta mostrar que u e v são não nulos. Se u=0 teríamos $-Dv^2 = 1$, um absurdo. Se v=0,viria u=1 ou -1.

De (*) seguiria que $\left(x_1 - y_1\sqrt{D}\right)\left(x_2 + y_2\sqrt{D}\right) = \pm m$, e assim

$\left(x_1 + y_1\sqrt{D}\right) = \pm\left(x_2 + y_2\sqrt{D}\right)$

Donde por fim $|x_1| = |x_2|$ o que é um absurdo.

OBS: Também com poucas modificações podemos tratar a equação

$(x^2 - Dy^2 = -1)$.

Exemplos:

1-Determinar todas as soluções inteiras não nulas das equações:

a) $x^2 - 2y^2 = 1$;

b) $x^2 - 5y^2 = 1$

Resoluções:

a) O teorema3.2.1,ensina que as soluções positivas dessa equação são da forma (x_n, y_n), onde x_n, y_n são os únicos inteiros para os quais

$x_n + y_n\sqrt{2} = \left(x_1 + y_1\sqrt{2}\right)^n$ *sendo* (x_1, y_1) a solução positiva para a qual $x_1 + y_1\sqrt{2}$ é o menor possível.como os pares (x,y)=(1,1),(1,2),(2,1),(2,2),(2,3) não são soluções da equação e (3,2) é ,é fácil nos convencermos de que (x_1, y_1) =(3,2).Desse modo ,temos os pares (x_n, y_n)dados pela igualdade $x_n + y_n\sqrt{2} = \left(3 + 2\sqrt{2}\right)^n$

b) Escrevendo-a na forma $\frac{x^2 - 1}{5} = y^2$ e dando a x os valores 1,2,3, …vê-se que o primeiro valor de x que torna $\frac{x^2 - 1}{5}$ quadrado perfeito é x=9,dando a y o valor 4.Esta é a solução mínima pois que qualquer outra terá para x e para y valores superiores a 9 e 4 respectivamente tornando $x - \sqrt{5}y$ superior a $9 + \sqrt{5}.4$.

A solução geral é dada por

$$x_n + y_n\sqrt{5} = \left(9 + 4\sqrt{5}\right)^n$$

ou

$$x = \frac{1}{2}\left[\left(9 + \sqrt{5}.4\right)^n + \left(9 - \sqrt{5}.4\right)^n\right]$$

$$y = \frac{1}{2\sqrt{5}}\left[(9 + \sqrt{5}.4)^n - \left(9 - \sqrt{5}.4\right)^n\right]$$

Por exemplo para n=2 obtemos x=161,y=72

Dada a equação $x^2 - Dy^2 = m$ (7)

onde m é inteiro qualquer.

É claro que no caso m=0 a equação não admite soluções além da trivial x=y=0,pois se esse fosse o caso teríamos x e y não nulos, e daí $\sqrt{D} = \frac{x}{y}$, um racional.

Lema 5.2.1. Seja ξ um irracional qualquer. Existem infinitos racionais $\frac{x}{y}$, com x e y inteiros não nulos, primos entre si, tais que $\left|\frac{x}{y} - \xi\right| < \frac{1}{y^2}$

Lema 5.2.2. Seja D um inteiro positivo que não seja quadrado perfeito, existe um inteiro m para o qual a equação $x^2 - Dy^2 = m$ admite infinitas soluções inteiros.

Demonstração . Sendo $\sqrt{D}$ um irracional, segundo a hipótese do lema, e o conjunto dos pares (x, y)de inteiros primos entre si tais que $\left|\frac{x}{y} - \sqrt{D}\right| < \frac{1}{y^2}$ é infinito com x e y satisfazendo (7), obtemos:

$$= \frac{1}{|y|}\left|\frac{x}{y} - \sqrt{D}\right|.\left|x + \sqrt{D}y\right| < \frac{1}{|y|}.\frac{1}{y^2}.\left|x + \sqrt{D}y\right| <$$

$$< \left|x + \sqrt{D}y\right| = \left|x - \sqrt{D}y + \sqrt{D}y + \sqrt{D}y\right| =$$

$$= \left|\left(x - \sqrt{D}y\right) + 2\sqrt{D}y\right| < \left|x - \sqrt{D}y\right| + \left|2\sqrt{D}y\right| <$$

$$< 1 + \left|2\sqrt{D}y\right|, \qquad \left(y \in Z \to \frac{1}{y}, \frac{1}{y^2} < 1\right)$$

Isto é

$$\left|x^2 - Dy^2\right| = |m| < 1 + \left|2\sqrt{D}y\right|$$

$$\Leftrightarrow -\left(1 + \left|2\sqrt{D}y\right|\right) < m < \left(1 + \left|2\sqrt{D}y\right|\right)$$

$$y = 1\, e\, \exists m \in Z : -1 - 2\sqrt{D} < m < 1 + 2\sqrt{D}$$

Donde segue que algum inteiro não nulo m entre $\left(-\left(2\sqrt{D}+1\right)\right) e \left(2\sqrt{D}+1\right)$ se repete um numero infinito de vezes, ou seja, há uma infinidade de números que substituídos em x e y torna $x^2 - Dy^2$ igual ao mesmo numero inteiro m, com $-2\sqrt{D} - 1 < m < 2\sqrt{D} + 1$. Isto significa que a equação $x^2 - Dy^2 = m$ admite infinitas soluções.

VI

EQUAÇÕES DE N-ÉSIMO GRAU (ÚLTIMO TEOREMA DE FERMAT):

$$x^n + y^n = z^n \qquad (1)$$

Já determinamos antes as equações de Pitágoras, nada mais natural que tentar estudar a equação mais geral do tipo $x^n + y^n = z^n$.

Fermat afirmou que a equação (1) não tem solução não trivial (isto é diferentes da solução x=y=0) para $n \geq 3$.

Nunca foi encontrada a demonstração que Fermat teria entre os papeis que legou.Até hoje ninguém conseguiu descobrir nenhuma demonstração geral embora se saiba que a afirmação de Fermat é verdadeira para inúmeros casos.

Para estudar o caso quando n é múltiplo de 4 vamos utilizar o método chamado de descida infinita, que desempenha um papel importante no estudo de equações com coeficientes inteiros.

Teorema 6.1. A equação $x^4 + y^4 = z^2$ não é solúvel em Z.

Demonstração. Por absurdo, suponhamos que existem inteiros positivos x,y,z tais que $x^4 + y^4 = z^2$ .Podemos também supor que x,y e z foram escolhidos de tal modo que

não há outra solução positiva a,b,c com c<z(aqui vamos usar o método da descida).Então x e y são primos entre si, e o teorema sobre os ternos Pitagóricos garante a existência de inteiros positivos primos entre si u e v tais que $x^2 = u^2 - v^2, y^2 = 2uv, z = u^2 + v^2 como\ x^2 + v^2 = u^2$, segue novamente do mesmo teorema dos ternos pitagóricos a existência de inteiros positivos primos entre si p e q tais que.

$x = p^2 - q^2, v = 2pq, u = p^2 + q^2$

Mas aí $y^2 = 2uv = 4pq(p^2 + q^2)$

Como p e q são primos entre si, teremos que ambos são também primos com $p^2 + q^2$. Portanto, sendo $4pq(p^2 + q^2)$ um quadrado devemos ter p, q e $p^2 + q^2$ quadrados, digamos $p = \alpha^2, q = \beta^2, p^2 + q^2 = \sigma^2, com\ \alpha, \beta, \sigma$ positivos.Por fim, segue que $\alpha^4 + \beta^4 = \sigma^2$ com $z = u^2 + v^2 > u = p^2 + q^2 = \sigma^2 \geq \sigma$, contrariando a minimualidade de z.

Logo, não há soluções não nulos de $x^4 + y^4 = z^2$.

Corolário 6.1. Se n for múltiplo de 4 então não existem inteiros não nulos x, y, z tais que $x^n + y^n = z^n$.

Demonstração. Seja n=4k, k natural.Se $x^n + y^n = z^n$, então teremos $\left(x^k\right)^4 + \left(y^k\right)^4 = \left(z^{2k}\right)^2, ou\ seja\ \left(x^k, y^k, z^{2k}\right)$ será uma solução da equação $a^4 + b^4 = c^2$.Assim, sabendo que essa última equação não admite soluções não nulas (**teorema 6.1**).Logo não há soluções não nulas de $x^n + y^n = z^n$ quando n for múltiplo de 4.

Em 1770, o suíço Euler provou o teorema para o caso n =3,que é bastante difícil do que o caso n=4.

Note-se que, depois de provado o teorema no caso n=4,basta estudar o caso em que o expoente é um primo ímpar. Isto pela razão seguinte:

Consideremos um expoente n qualquer maior que 2.Se n for um múltiplo de 4, digamos n=4k, então a equação $x^n + y^n = z^n$ não tem certeza soluções inteira.

Se n não for um múltiplo de 4, n é de certeza divisível por um primo ímpar p,digamos n=qp.

Se a equação $x^n + y^n = z^n$ tiver soluções inteiras, também a equação com expoente p as tem ,pois sendo n=qp a equação $x^n + y^n = z^n$ é equivalente a $\left(x^q\right)^p + \left(y^q\right)^p = \left(z^q\right)^p$.

Basta portanto estudar o caso em que o expoente é um primo ímpar.

No século XIX, vários matemáticos foram provando o teorema para expoentes cada vez maiores.

O alemão Dirichlet provou em 1825 que o teorema vale para n=5.

O francês Lamé provou em 1839 que o teorema vale para n=7.

O alemão kummer introduziu técnicas algébricas novas que permitiram provar o teorema para outros valores de n.

No século XX muitos autores publicaram demonstrações erradas do resultado geral.

Em 1983,o alemão Faltings (então com 29 anos) provou que, para cada n maior que 2, a equação $x^n + y^n = z^n$ tem no máximo um numero finito de soluções (trios de inteiros em que os números são primos entre si), o que foi um grande progresso no sentido da demonstração de resultado geral, que afirma que esse numero é zero. Usando técnicas baseadas no trabalho de Kummer, em 1993 provou-se, com a ajuda de computadores, que o teorema é valido para todos os expoentes $n \leq 4000000$.

Finalmente, em 1995,o inglês Wiles, num trabalho extenso e difícil, demonstrou que o ultimo teorema de Fermat é verdadeiro (para todos os expoentes n maior que 2). Os resultados e técnica utilizados mostram que o ultimo teorema de Fermat não e uma curiosidade isolada da teoria dos números, mas tem relação profundas com muitos outros importantes temas da

Matemática.

VII

CONCLUSÃO

Ao longo deste trabalho, tentamos fazer uma abordagem sobre as principais equações em Z.

No entanto para melhor compreensão do tema tivemos que recorrer à alguns conceitos preliminares (fracções continuas) e alguns teoremas. Prova disto são os exercícios demonstrativos em vários capítulos, que nos ajudam a resolver no nosso dia a dia problemas ligados com a álgebra em particular e a matemática em geral.

O presente trabalho pode ser tomado como mais um elemento complementar ás sugestões da teoria dos números. Possivelmente será um elemento de análise aos alunos que pretendem continuar o seu percurso a nível superior apesar de ter algumas ligações com o ensino secundário.

Com esse trabalho concluímos sobre:

-A importância do teorema de Pitágoras na resolução de equações e que para encontrar os ternos Pitagóricos existe uma técnica que consiste em:

1. Escolher um número ímpar;
2. Elevá-lo ao quadrado;
3. Decompor este quadrado em soma de dois números consecutivos;

$$n^2 = \frac{1}{2}\left(n^2 - 1\right) + \frac{1}{2}\left(n^2 + 1\right)$$

A tabela seguinte poderá ajudar na procura de ternos pitagóricos

n	n^2	$\frac{1}{2}\left(n^2-1\right)$	$\frac{1}{2}\left(n^2+1\right)$
3	9	4	5
5	25	12	13
7	49	24	25
9	81	40	41
…	…	…	…

-As relações entre as equações em Z com muitos outros importantes temas da matemática

-A grande ligação entre as fracções continuas e as equações em Z

-Os vários métodos para a resolução da equação do tipo $x^2 - Ay^2 = 1$

Para resolver essas equações podemos:

1º-Por meio de fracções contínuas encontrar as soluções mínimas que são:

$$x_0 = P_{k-1} \quad , y_0 = Q_{k-1} \qquad se\ k - par$$
$$x_0 = P_{2k-1} \quad , y_0 = Q_{2k-1} \qquad se\ k - impar$$

k-comprimento da decomposição de $\sqrt{A}$ em fracções contínuas

2º- Por meio do teorema 5.2.1 em que as soluções podem ser da forma:

$x_n + y_n\sqrt{A} = \left(x_1 + y_1\sqrt{A}\right)^n \quad \left(n \in N \setminus \{0\}\right)$ e

$x_n - y_n\sqrt{A} = \left(x_1 - y_1\sqrt{A}\right)^n$

Ainda do mesmo teorema as soluções podem ser da forma:

$$x_n = \frac{1}{2}\left[\left(x_1 + \sqrt{A}y_1\right)^n + \left(x_1 - \sqrt{A}y_1\right)^n\right]$$

$$y_n = \frac{1}{2\sqrt{A}}\left[\left(x_1 + \sqrt{A}y_1\right)^n - \left(x_1 - \sqrt{A}y_1\right)^n\right]$$

Onde (x_1, y_1) são soluções mínimas e (x_n, y_n) uma solução qualquer

-A relação entre o ultimo teorema de Fermat e as equações de Pitágoras

VIII

RECOMENDAÇÕES

Com efeito, tudo o que foi dito e demonstrado ao longo desse trabalho e com as conclusões tiradas, gostaríamos de apresentar algumas recomendações que poderão, seguramente servir de suporte e ajuda na melhoria do ensino aprendizagem desse tema tanto a nível do Ensino Secundário como a nível do Ensino Superior:

1. Que o presente trabalho, como outros, constitua uma mais valia no ensino de equações;
2. Que os professores do ensino secundário utilizem não só o método geométrico na resolução de equações lineares mas também métodos algébricos;
3. Que a nível superior não se resolvam equações usando apenas a noção de fracções próximas;
4. Que haja manuais disponíveis, munidos de vários métodos da resolução de equações;

IX

BIBLIOGRAFIA

1. A.A.Burstab-´´teoria dos números ``, Moscovo, 1966;

2.JAHH,M.Convay;RICHARD, K.Guy-´´O Livro dos Números ``-tradução José Sousa Pinto;

3. L.I.Burevitch, I.R.Chafarevitch-´´Théoria des Nombres``, Éditions Jacques Gabay, Paris, 1967;

4.NEVES,Maria Augusta Ferreira; FARIA, Maria Luísa Monteiro-´´Matemática 9º ano de escolaridade-Livro de Texto IIº volume``, Porto Editora, Porto, 1995;

5.OLIVEIRA,Graciano Neves -´´Resolução de Equações em Números Inteiros``-I Escola de Verão, Coimbra, 1981;

6.V.V.Ostrik;M.A.Tcfasman-´´Geometria Algébrica e Teoria dos Números: Curvas elípticas e Racionais``-Moscovo, 2001´´Biblioteca da educação matemática ``.

7.Equaçoes diafantinas – Disponível em < http://www.mat.uc.pt/~jqueiro/TN8.pd>. Acesso em: 20 nov.2005

8.Equaçoes diafantinas-Disponivel em <http://www.terra.com.br/eureka/artigos/diofantinas.doc.> Acesso em: 10 dez.2005

Anexos

EXERCICIOS PROPOSTOS:

CAPÍTULO II

2.1-Reduzir as fracções:

a) $-\frac{53}{17}$;

b) $\frac{220}{315}$;

2.2-Encontrar a terceira fracção próxima à fracção contínua do número $\frac{92}{21}$

CAPÍTULO III

3.1-Resolver em Z as equações seguintes de duas maneiras diferentes:

a) 2x+3y =6

b) 9x+11y=-7

CAPÍTULO IV

4.1-Descrever todas as soluções inteiras das equações.

a) $x^2 - 15y^2 = z^2$;

b) $x^2 + 4y^2 = 5z^2$;

4.2-Demostrar que o número 7 é um número congruente

CAPITULO V

5.1-Descrever todas as soluções inteiras não nulas das equações:

a) $x^2 - 7y^2 = 1$

b) $x^2 - 2y^2 = -1$

CAPITULO VI

6.1-Mostrar que as equações a seguir não possuem soluções inteiras não nulas:

a) $x^4 + 4y^4 = z^2$;

b) $x^4 + 2y^4 = z^2$;

SOLUÇÕES /SUGESTÕES:

2.1.

a) $[-3;8,3]$

b) $[0;1,2,3,6]$

2.2.

$\frac{92}{21}=[4;2,1,1,1,2]$

$\frac{P_3}{Q_3}=\frac{22}{5}$

3.1

a) X=-6-3t
Y=6+2t $\quad t\in Z$

b) x=-35-11t
y=28+9t $\quad t\in Z$

4.1

a)

$x=(15m^2+n^2)r$

$y=2mnr$

$z=\left(15m^2-n^2\right)r$

b)

$x=(-m^2+10mn-5n^2)r$

$y=\left(m^2-5n^2\right)r$

$z=\left(m^2-2mn+5n^2\right)r$

4.2

Sugestão:

É fácil ver que se s é um numero congruente, então sl^2 também, é, para $\forall l\in$ □ .Pois o triangulo que tem área igual a sl^2 obtém-se do triângulo da área s por aumento de todos os lados em l vezes.

Assim como $\frac{m}{n}=m.n.\frac{1}{n^2}$, podemos, no futuro, considerar só números livres dos quadrados.

5.1

a)

$$x = \frac{1}{2}\left[\left(9+\sqrt{7}.4\right)^n + \left(9-\sqrt{7}.4\right)^n\right]$$

$$y = \frac{1}{2\sqrt{7}}\left[\left(9+\sqrt{7}.4\right)^n - \left(9-\sqrt{7}.4\right)^n\right]$$

b)

$$x = \frac{1}{2}\left[\left(1+\sqrt{2}\right)^n + \left(1-\sqrt{2}\right)^n\right]$$

$$y = \frac{1}{2\sqrt{2}}\left[\left(1+\sqrt{2}\right)^n - \left(1-\sqrt{2}\right)^n\right]$$

6.1

Sugestões

De acordo com o teorema 6.1do capítulo VI as equações do tipo $x^4 + y^4 = z^2$ não possuem soluções inteiras. Sabendo que as equações das alíneas a) e b) podem ser escrita nessa fórmula logo não possuem soluções inteiras.